

# Exhibit 2

Derek W. Loeser (admitted *pro hac vice*)  
KELLER ROHRBACK L.L.P.  
1201 Third Avenue, Suite 3200  
Seattle, WA 98101  
Tel.: (206) 623-1900  
Fax: (206) 623-3384  
dloeser@kellerrohrback.com

Lesley E. Weaver (SBN 191305)  
BLEICHMAR FONTI & AULD LLP  
555 12th Street, Suite 1600  
Oakland, CA 94607  
Tel.: (415) 445-4003  
Fax: (415) 445-4020  
lweaver@bfalaw.com

*Plaintiffs' Co-Lead Counsel*

*Additional counsel listed on signature page*

**UNITED STATES DISTRICT COURT  
NORTHERN DISTRICT OF CALIFORNIA**

IN RE: FACEBOOK, INC. CONSUMER  
PRIVACY USER PROFILE LITIGATION

MDL No. 2843  
Case No. 18-md-02843-VC

This document relates to:

ALL ACTIONS

**PLAINTIFFS' OPPOSITION TO  
DEFENDANT FACEBOOK, INC.'S  
REQUEST TO ENFORCE THE PARTIAL  
STAY OF DISCOVERY IN PRETRIAL  
ORDER NO. 20 AND CROSS-MOTION  
TO COMPEL DISCOVERY RELATED  
TO REQUESTS FOR PRODUCTION  
NOS. 9 THROUGH 13**

Judges: Hon. Vince Chhabria  
Hon. Jacqueline S. Corley  
Courtroom: 4, 17th Floor

## TABLE OF CONTENTS

I.	INTRODUCTION .....	1
II.	ARGUMENT .....	2
	A.    The Order does not limit discovery to users' platform activity.....	2
	B.    The discovery requests at issue and Facebook's response .....	6
	C.    Relevant sensitive information is not limited to platform activity, but also includes sensitive information Facebook derives and collects from business partners, app developers, apps, and other sources. ....	7
	1.    User data includes, in Facebook's words, "native, appended and behavioral data" that Facebook collects from business partners, apps and other activity .....	8
	2.    Internal documents confirm that Facebook's description of data "associated" with users is misleading.....	11
	D.    Facebook has not established that the burden of producing the data relating to ten Plaintiffs is disproportional to the needs of this case .....	12
III.	CONCLUSION .....	14

**TABLE OF AUTHORITIES**

	<b>Page(s)</b>
<b>Cases</b>	
<i>Doe v. Gangland Prods., Inc.,</i> 730 F.3d 946 (9th Cir. 2013) .....	10
<i>Harris v. Best Buy Stores, L.P.,</i> No. 3:15-cv-00657-HSG (KAW), 2016 WL 6024556 (N.D. Cal. Oct. 14, 2016).....	13
<i>Polaris Innovations Ltd. v. Kingston Tech. Co.,</i> No. CV1600300CJCRAOX, 2017 WL 3275615 (C.D. Cal. Feb. 14, 2017).....	14
<i>Shulman v. Grp. W. Prods., Inc.,</i> 18 Cal.4th 200 (1998).....	10
<i>SPS Techs., LLC v. Briles Aerospace, Inc.,</i> No. CV 18-9536 MWF, 2020 WL 4341717 (C.D. Cal. June 25, 2020) .....	14
<i>Sullivan v. Personalized Media Commc'ns, LLC,</i> No. 16-MC-80183-MEJ, 2016 WL 5109994 (N.D. Cal. Sept. 21, 2016) .....	14
<b>Statutes</b>	
18 U.S.C. § 2702(a) .....	3, 4, 5, 10
18 U.S.C. § 2710(b)(2).....	3, 4, 5, 10
<b>Other Authorities</b>	
Fed. R. Civ. P. 26(b)(1).....	13
Local Rule 5-1(i)(3) .....	16

## I. INTRODUCTION

Facebook does not want Plaintiffs to obtain discovery showing the full breadth of its wrongful disclosure of its users' sensitive information. Accordingly, Facebook seeks to limit discovery in this case to a single category of improperly shared information: users' activity on the Facebook platform. The sensitive information that Facebook collects and shares with third parties is much more extensive than this. It collects users' sensitive information from a variety of sources—including from third parties—then pools the information with user-posted activity and generates additional information from the full data set it accumulates. It then shares this information about users and their friends with third parties. All of this information, including who has access to it and how it is used, is relevant to Plaintiffs' claims.

As a result, there are at least three compelling reasons that Facebook's motion should be denied and Plaintiffs' cross-motion to compel production of documents responsive to Requests for Production ("RFPs") Nos. 9 through 13<sup>1</sup> should be granted.

*First*, contrary to Facebook's tortured reading of Pretrial Order No. 20 ("Order" or "PTO 20"), Dkt. No. 298, the Court did not limit discovery in this case only to information regarding user activity on Facebook. While that information—and Facebook's subsequent disclosure of it—is of course relevant, that is not the only type of sensitive information relevant to Plaintiffs' claims or the four categories of wrongdoing recognized by the Order.

*Second*, the universe of data Facebook collects and shares about users is also not limited to user activity on Facebook, but instead consists of a sea of information obtained from a wide variety of sources, including from business partners, app developers, apps, and other third parties. Indeed, as Facebook's own documents show, it collects information about users far beyond what Facebook has produced in this case. And discovery produced to date further confirms that Facebook not only collects this information, but links it to users and shares it with third parties—putting to rest Facebook's nonsensical suggestions that Plaintiffs have failed to articulate what additional evidence exists or that Facebook cannot "associate" certain data with a

---

<sup>1</sup> For details on these RFPs, see *infra* § II.B.

user.

*Third*, there is no justification for Facebook’s claims of undue burden. Such an argument should be accorded minimal weight in a case of this size and complexity involving a company whose business model is premised upon the collection and production of electronic information about billions of users. Facebook has come nowhere near meeting its burden of demonstrating why data regarding solely Named Plaintiffs—relative to the hundreds of millions of potential class members whose information is ultimately at issue in this case—is not proportional to the needs of the case. In fact, pursuant to the Court’s recent guidance regarding streamlining Plaintiffs’ discovery, Plaintiffs have reduced the number of individuals who will be class representatives to ten, down from the twenty-three. Plaintiffs only seek the discovery at issue here related to these ten Plaintiffs (for purposes of this motion, the “Named Plaintiffs.”)

## II. ARGUMENT

### A. The Order does not limit discovery to users’ platform activity.

PTO 20 does not directly address the question raised by Facebook in its motion—whether this case is limited to user activity on the Facebook platform or includes all the sensitive information about users that Facebook improperly shared with third parties. But the Order nowhere expressly limits the case to user activity. *Cf. Mot.*<sup>2</sup> at 1. Nor does it make sense to read the Order that way. That sort of limitation would conflict not only with claims and theories that the Order upheld, but also with the grounds on which they were allowed to proceed to discovery.

Facebook, under the guise of enforcing a discovery stay that was never issued in the first place, spends many pages straining to read the Order to limit discovery to data relating only to users’ on-platform activity. This provides a misleading picture of what the Order says and inaccurately ascribes to the Court a set of internally inconsistent views.

**1. The Order.** The Order summarizes its understanding of Plaintiffs’ claims in a two-sentence précis near the beginning: “Broadly speaking, this case is about whether Facebook

---

<sup>2</sup> Def. Facebook, Inc.’s Opening Brief in Supp. of Its Req. to Enforce the Partial Stay of Discovery in Pretrial Order No. 20 (“Mot.”), Dkt. No. 515.

acted unlawfully in making user information widely available to third parties. It's also about whether Facebook acted unlawfully in failing to do anything meaningful to prevent third parties from misusing the information they obtained.” Order at 3. This description focuses on *Facebook's* unlawful disclosure of information about users and their friends to third parties—not on whether that information was originally posted, shared, or generated by users on the Facebook platform.

The Order then discusses the four categories of Facebook's wrongdoing. These categories are: (1) “[g]iving app developers access to sensitive user information”; (2) “[c]ontinued disclosure to whitelisted apps”; (3) “[s]haring sensitive user information with business partners”; and (4) “[f]ailure to restrict the use of sensitive information.” Order at 6-9. These categories line up neatly with the earlier description of the action as alleging that “Facebook acted unlawfully in making user information widely available to third parties” (the first three categories) and that Facebook “fail[ed] to do anything meaningful to prevent third parties from misusing the information they obtained” (the fourth category). *Id.* at 3.

Using these four categories of wrongdoing as a framework, the Order analyzed whether Plaintiffs had standing to bring their claims and whether they stated valid claims. It ruled that Plaintiffs had standing because they alleged that their “sensitive information was disseminated to third parties in violation of their privacy.” *Id.* at 14. It upheld nearly all of Plaintiffs' claims (e.g., three privacy-based tort claims under California law, a claim under the Stored Communications Act (“SCA”), a claim for breach of contract, and a claim for unjust enrichment) except to the extent they were based on the first category of wrongdoing, the disclosure of user information to app developers. *Id.* at 30-34, 38-41. It upheld in its entirety Plaintiffs' claim under the Video Privacy Protection Act (“VPPA”). *Id.* at 34-35. And it upheld Plaintiffs' claim for negligence, which was based on the fourth category of wrongdoing. *Id.* at 35-36.

**2. *The Order's rationale.*** Why did the Order conclude that Plaintiffs had standing and had stated valid claims? On these points, the Order is clear. Plaintiffs had standing because “their “sensitive information was disseminated to third parties in violation of their privacy.” *Id.* at 14.

This reasoning focuses not on *where* the user information was originally generated—whether on the Facebook platform or off it—but on its nature (“sensitive”) and on what Facebook did with it (“disseminated” it “to third parties”).

Similarly, when discussing the claims, the Order focused not on the original provenance of the information about users, but on its nature and on what Facebook did with it. So, for example, the Order ruled that:

- Plaintiffs had stated valid privacy torts because Facebook had disseminated information that was “sensitive” and as to which Plaintiffs had a reasonable expectation of privacy. *Id.* at 30-33.
- Plaintiffs had stated a claim under the Stored Communications Act because Facebook had disseminated the content of their electronic communications and had not gained their consent to do so. *Id.* at 33-34.
- Plaintiffs had stated a claim under the Video Privacy Protection Act because Facebook had disseminated “information which identifies a person as having requested or obtained specific video materials or services,” *id.* at 34 (citation omitted), and Facebook qualified as a “video tape services provider” under the statute, *id.* at 35.

### **3. “Sensitive information” is not defined by where Facebook collects that information.**

The Order repeatedly notes that Facebook shares “sensitive” user information without consent. Facebook pins its argument to this one word, maintaining that the Order “defined” sensitive user information to mean only information about what users post on Facebook, Mot. at 1, or users’ platform activity, Mot. at 8. But the common-sense meaning of “sensitive information” encompasses more than just what users did on the platform. Consider, for example, a Facebook user’s Amazon.com order for an over-the-counter contraceptive or another user’s entry of “alcoholic support group in Tower District, Fresno” into a search engine. “Sensitive information” also includes information that Facebook can *infer* from on-platform information—a category of information it has not produced. (Think of the inferences that Facebook can draw from weekly photographs of a user taken at M.D. Anderson Cancer Center.) Facebook’s objection that such information is categorically not “sensitive” is false.

It is true that when the Order gave examples of sensitive user information, the examples it

used concerned information generated on the Facebook platform. *E.g.*, Order at 1, 17. Nowhere, however, did the Order *define* or *limit* sensitive information to users' platform activity only. And the Order's reasoning certainly is not limited to such information. Rather, as noted above, Plaintiffs' standing to bring their claims, and the validity of many of those claims, depends on the nature rather than the provenance of the information, and on whether Facebook shared that information with third parties. And, as Plaintiffs have learned through discovery, the sensitive information about users that Facebook collects and shares with business partners and app developers includes both information originally generated outside the Facebook platform and information derived from on- and off-platform activity.

It also is farfetched for Facebook to argue that the Order rules that *all* of Plaintiffs' claims—including their federal statutory claims—rise or fall depending on whether the information that Facebook shared is “sensitive” in the sense of being embarrassing or deeply intimate. The validity of Plaintiffs' claim under the SCA, for example, does not turn on how embarrassing or intimate the information is that Facebook shared, but on whether the shared information includes the contents of an electronic communication. 18 U.S.C. § 2702(a)(1). Similarly, Plaintiffs VPPA claim turns on whether the information that Facebook shared includes “information which identifies a person as having requested or obtained specific video materials or services from a video tape service provider.” *Id.* § 2710(a)(3). If, for example, Facebook collected and shared a user's video-watching queue from a different platform, that would constitute a VPPA violation.

In sum, while the Order does not explicitly address the issue posed by Facebook's motion, it certainly does not limit discovery in this case to on-platform user activity and reading it that way is inconsistent with the Court's reasoning. It is also inconsistent with statements by the Court during the motion to dismiss hearing about the breadth of user data that is relevant to Plaintiffs' claims:

For example, if – I'm a Facebook user. And, you know, I'm trying to assess the likelihood that my sensitive information got into the hands of third parties and, if so, how many third parties and, if so, what kinds of third parties. If I have a full

understanding of the third parties that had access to the information, and a full understanding of what type of information they had access to, and a full understanding of who they were, and what they – and what restrictions were placed on them, we then have a better understanding of what was likely to have happened to me.

Nov. 4, 2019 Tr. at 15:20-16:4. It is the “full understanding” referred to by the Court that Plaintiffs seek, and that Facebook refuses to allow.

Finally, this reading prevents Named Plaintiffs from discovering even the general policies and practices of Facebook governing the sharing of their sensitive information, policies and practices that are critical for this case. *See* Pretrial Order No. 30 at 2, Dkt. No. 347 (“[T]he best way to assess the merits and to determine whether class certification is appropriate is almost certainly to conduct discovery on Facebook’s general practices.”). Plaintiffs submit that Facebook’s exclusion of this information from discovery is not what the Order intended.

**4. *The Order stayed claims, not discovery.*** Plaintiffs organized their claims into three categories: prioritized claims, prioritized consumer protection act claims alleged in the alternative, and non-prioritized claims. First Am. Consolidated Compl. (“FACC”) at 317-411, Dkt. No. 257. The Order made the simple observation that “[a]ll other prioritized claims not addressed by this ruling will be stayed (effectively, relegated to non-prioritized status) and adjudicated, if necessary, at a later state in the proceedings with the other non-prioritized claims.” Order at 6. Facebook’s claim that this holding somehow imposed a stay of *discovery* is baffling. The Order does not, and does not purport to, stay discovery in any fashion.<sup>3</sup>

#### **B. The discovery requests at issue and Facebook’s response**

The present dispute arises from five discovery requests, each of which asks for data that Facebook possesses about Named Plaintiffs, the third parties that Facebook disclosed this data to, and the types of information that was disclosed to them. *See* Ex. A, Def. Facebook, Inc.’s Resp. & Obj. to Pls.’ Second Set of Reqs. for Produc. In particular, RFP No. 9 requests “[a]ll

---

<sup>3</sup> Even if it were, the Order observed that “[o]f course, dismissal of a subset of claims with prejudice does not preclude a plaintiff from seeking revival if discovery reveals a factual basis that justifies reconsideration[.]” Order at 37 n.21 (citations omitted).

Documents relating to each of the Named Plaintiffs, including but not limited to all Content and Information collected about each of them or gained from business relationships or any other source.”<sup>4</sup> *Id.* RFP No. 10 asks Facebook to produce, “[f]or each of the Named Plaintiffs, Documents sufficient to show the categories of Content and Information Facebook collects, tracks, and maintains about them.” *Id.* RFP Nos. 11-13 then request documents requesting Facebook to identify the third parties that were able to access this information, including the categories of data that were disclosed to them and how they accessed it. *Id.* Plaintiffs propounded these requests nearly one year ago in November 2019.

In response to these requests, Facebook produced information collected by the DYI (“Download Your Information”) tool. This limited tool allows downloads of some, but not all, information relating to users’ activity on the platform. And Facebook freely acknowledges that Plaintiffs can access this information themselves. *Id.* (“[A]ll Facebook users are free to download their DYI file if they wish.”). In addition to the DYI production, Facebook has produced an undefined category of “additional information associated with [users’] accounts” for each Plaintiff. Mot. at 6. But Facebook does not describe what the “additional information” is, likely because it is extremely limited—it consists solely of information users can access through their account in the form of their privacy settings and information reflecting user activity on Facebook. Critically, the form of production also obscures whether some of the activity was public or private. Thus, virtually all of Facebook’s 850,000-page production relating to the original Named Plaintiffs in this case was already accessible to Plaintiffs and tells only part of the story.

**C. Relevant sensitive information is not limited to platform activity, but also includes sensitive information Facebook derives and collects from business partners, app developers, apps, and other sources.**

Facebook acknowledges that it collects and shares substantial amounts of additional sensitive information about users beyond their platform activity. *See, e.g.*, Aug. 14, 2020 Hrg

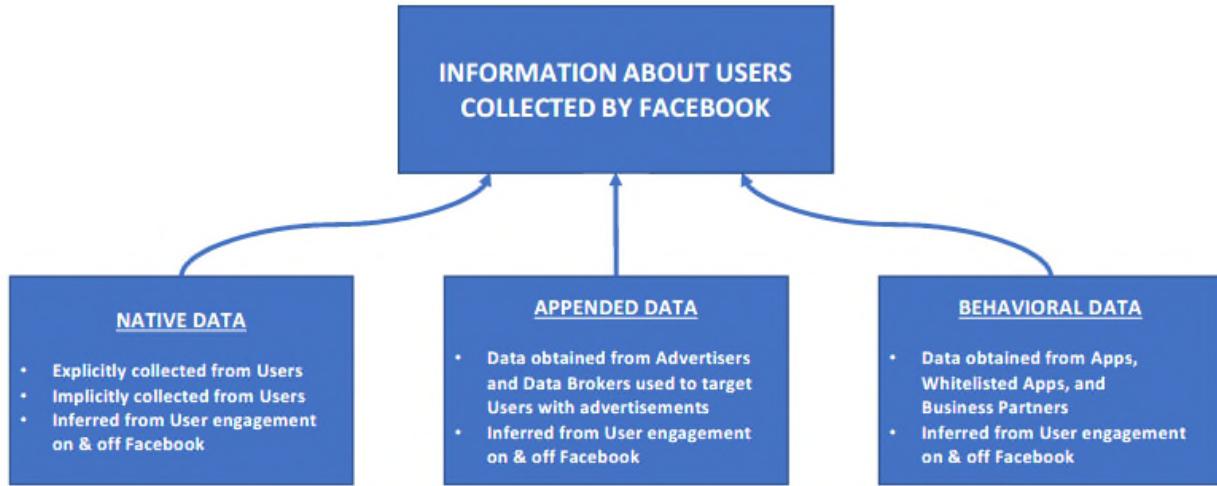
---

<sup>4</sup> The requests use the definition of “Content and Information” from Facebook’s Statement of Rights of Responsibilities—a definition that is not limited to on-platform data.

Tr. 8:10-13 (“[T]here’s Facebook-generated information, information generated by third parties, information received from third parties. We have not represented that that is comprehensively included in our production.”); *see also* Mot. at 10-15 (describing off-platform activity and internal analytics it has not produced). However, Facebook contends that this other information is not relevant to this case. This is false.

**1. User data includes, in Facebook’s words, “native, appended and behavioral data” that Facebook collects from business partners, apps and other activity.**

Facebook identifies three general categories of information it possesses about Facebook users: Native Data, Appended Data, and Behavioral Data. *See* Ex. B, FB-CA-MDL-00213424-439. Native Data includes public and private information Facebook collects from a user’s activity on Facebook such as a user’s profile info, posts, likes, shares, and location and device information. *Id.* Native Data also includes a small subset of information it can infer from user activity on and off Facebook, such as user interests and behaviors. *Id.* Appended and Behavioral Data, on the other hand, consists of information inferred from user activity on and off Facebook. Specifically, Appended Data is user information obtained from third parties, including advertisers and data brokers, about a user’s activities—*e.g.*, auto registration, retail and credit card purchase histories, as well as other “enhanced” customer databases. *Id.* Behavioral Data consists of substantial information related to users including their activity within third-party applications—*e.g.*, website browsing behavior, app installations, and purchases they make off the Facebook platform. *Id.* These three categories of information, and how Facebook obtains this information, are illustrated as follows:



While Native Data—the only type of data Facebook has partially produced about users so far—is important for this case, so too is Appended and Behavioral Data obtained from user “engagement” on and off the platform. Moreover, Facebook connects and integrates Native, Appended and Behavioral Data generated from on-platform activity with data obtained from third parties. *See Ex. B, FB-CA-MDL-00213424-439* (identifying Facebook’s matching of data it receives directly from users with Appended Data and Behavioral Data received from third parties through “[REDACTED]”); *id.* at FB-CA-MDL-00213424 (describing Facebook’s [REDACTED] process as instances where [REDACTED]).

Critically—and contrary to Facebook’s suggestion that this data is irrelevant and duplicative of information it has already produced (Mot. at 14)—discovery confirms that Facebook shares this data with third parties. For example, a 2012 internal email between senior team members explains that “Facebook has information about users which can be helpful to applications, and *which we provide to applications when we deem appropriate[.]*” Ex. C, Email from Sam Lessin to Douglas Purdy (Aug. 30, 2012), at 3 (emphasis added), NBCNews (Nov. 6, 2019), <https://dataviz.nbcnews.com/projects/20191104-facebook-leaked-documents/assets/facebook-sealed-exhibits.pdf> at 716. The email also identifies the kind of data

that Facebook shares, including (1) “[a]ggregate data about the tastes, properties, etc. of a user’s friends,” (2) “[d]erived data about a user/facebook’s data/opinion of a user (probably location, account trust score, account age, etc.),” and (3) “[d]ata provided by third parties – information which third parties have contributed to the graph on behalf of a user.” *Id.*

Another internal document, [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

These documents make clear that Facebook collects sensitive user information in a variety of different ways and discloses it to third parties.

Facebook’s insistence that it need only produce on-platform Native Data makes even less sense when considering Plaintiffs’ claims. Plaintiffs’ statutory and common law claims are not limited to information generated from users’ activities on Facebook. For example, under the VPPA, Plaintiffs must prove that Facebook disclosed “personally identifiable information concerning any consumer” to “any person” absent written or informed consent. 18 U.S.C. § 2710(b)(2). Under the SCA, Plaintiffs must prove that Facebook “knowingly divulge[d] to any person or entity the contents of any communication” users did not intend for Facebook to divulge. 18 U.S.C. § 2702(a). The source of the information—that is, whether it was the result of on- or off- platform activity, gleaned directly from users’ posts, or inferred from them—is irrelevant. Disclosure of any of this information without consent is actionable.

Similarly, Plaintiffs’ Public Disclosure of Private Acts claim requires Plaintiffs to prove that Facebook disclosed a private fact about the plaintiff that is objectionable and offensive to a reasonable person. *Doe v. Gangland Prods., Inc.*, 730 F.3d 946, 958 (9th Cir. 2013). Likewise, Plaintiffs’ Intrusion into Private Affairs claim requires Plaintiffs to prove an intrusion by Facebook into a private matter that is highly offensive to a reasonable person. *Shulman v. Grp. W. Prods., Inc.*, 18 Cal.4th 200, 231 (1998). In order to prove these claims, Plaintiffs must

ascertain the private facts about them that Facebook is collecting and disclosing, whether they originate from platform activity or not.

Across many claims, the Order sustained Plaintiffs' allegations about Facebook's undisclosed data reciprocity programs with business partners. Plaintiffs are thus entitled to know what sensitive user data, of any type or source, Facebook shared with its business partners. Plaintiffs are further entitled to any data that Facebook received from its business partners in return, since the value of that data constitutes the benefit Facebook received in the transaction, a benefit that Plaintiffs are entitled to recover under, *inter alia*, the unjust enrichment claim that the Court sustained. Order at 41;<sup>5</sup> *see also* Order at 8 (noting the allegation that "Facebook and its [business] partners agreed to exchange information about users' activities with each other").

Facebook notes repeatedly that targeted advertising and psychographic marketing are not part of this case. *See, e.g.*, Mot. at 9. This argument misses the point. The question is not whether Facebook should or should not have engaged in targeted advertising and psychographic marketing. The question is whether, when doing so, Facebook shared sensitive user and friend information without consent. Plaintiffs are entitled to obtain the discovery necessary to substantiate the allegation that improper sharing has occurred in the context of these activities.

**2. Internal documents confirm that Facebook's description of data "associated" with users is misleading.**

Facebook claims it has produced all data it possesses that is "associated" with Named Plaintiffs. That is, while it generated and collected reams of data about Named Plaintiffs, Facebook claims that most of that data, including Appended and Behavioral Data, is anonymized and cannot be connected to Named Plaintiffs. This is false.

Facebook explains that Appended and Behavioral Data cannot be associated with Plaintiffs' Facebook accounts because such data is "disassociated from the user's ID within 90

---

<sup>5</sup> Facebook's position blocking discovery of what it possesses and shares is in tension with Facebook's own discovery requests to Named Plaintiffs. Facebook's Interrogatory No. 8 asks Plaintiffs to "Identify all entities other than Cambridge Analytica that You believe have "misused sensitive information from Your Facebook Account." But Facebook itself will not identify with whom it shared that sensitive information, let alone what information it possesses.

days" (Mot. at 15). But, as confirmed by internal documents, what actually happens is that Facebook replaces the User ID, or "UID," with a Random ID, or "Replacement ID" or "RID"—and *stores the connection between a UID and an RID* until users delete their accounts.<sup>6</sup> In other words, Facebook replaces the User ID with another identifier, yet the data is still directly linked to and associated with a given user. Indeed, the very purpose of collecting all of this data in the first place is to use it to target users and their friends. Facebook can readily connect any active user with Appended Data and Behavioral Data containing that user's RID<sup>7</sup> and, thus, it can be easily searched for, identified, and copied, without "multiple operations . . . to try to determine whether any data in the analysis originated from a Named Plaintiff." *Cf.* Mot. at 15.

Similarly, Appended Data without a RID can be connected to active users through "[h]ashed data matching." *See* Ex. B. "Hashed data matching" is the process of matching different data sets through the hash values of unique identifiers. For instance, when an advertiser uploads a spreadsheet of Custom Audience data including hashed email addresses, Facebook can match this data to its users through the hashed email address field.

Thus, it simply is untrue that it would be "nearly impossible" to produce the "disassociated" data in this case for Named Plaintiffs. Mot. at 15. Facebook clearly has the ability to connect Named Plaintiffs' user information through RIDs and hashed data matching, and should be ordered to do so in response to RFP Nos. 9-13.

**D. Facebook has not established that the burden of producing the data relating to ten Plaintiffs is disproportional to the needs of this case.**

Facebook also suggests that "the burdens of locating the additional information Plaintiffs seek would far exceed the needs of the case." Mot. at 12. But the burden associated with producing the requested information is not undue; it is proportional to the needs of this complex

---

<sup>6</sup> Ex. E, PwC\_CPUP\_FB00030737-738.

<sup>7</sup> *Id.* at PwC\_CPUP\_FB00030738 [REDACTED]

case. In assessing proportionality, Federal Rule of Civil Procedure 26 directs consideration of “the importance of the issues at stake in the action, the amount in controversy, the parties’ relative access to relevant information, the parties’ resources, the importance of the discovery in resolving the issues, and whether the burden or expense of the proposed discovery outweighs its likely benefit.” Fed. R. Civ. P. 26(b)(1). Helpfully, Judge Chhabria provided further guidance at the March 5, 2020 Case Management Conference, stating:

I am concerned that Facebook has, you know, often made statements reflecting an unduly narrow view of what should be turned over to the Plaintiffs. And, you know, this is a big case. I mean, there is often a lot of talk about proportionality and whatnot. This is a big case. It is a significant issue. You know, and there is -- this is not the type of case where we are going to be saying: Well, that might end up -- that effort might end up uncovering some relevant information; but, you know, it is just too expensive or difficult, and so we are not going to make Facebook do it. This is really not one of those cases where that is very -- that type of argument is likely to carry the day. You know, and, as I have said a number of times, you know, the best way to figure out what happened as it relates to the claims that are going forward now is to -- for Facebook to produce all information, all documents about the practices associated with giving third parties access to friends' information and friends' of friends information.

Tr. at 28:25-29:18. Judge Chhabria’s observations regarding the size of this case remain on point. The proposed class period extends from 2007 to the present, the potential class members number in the hundreds of millions, and the third parties with whom Facebook shared user data appear to number in the tens of thousands. In that context, Plaintiffs’ request for the data concerning ten individual users seems not only proportional to the needs of the case but modest.

Furthermore, Facebook’s claims of burden are unsupported. “[T]he party opposing discovery has the burden of showing that discovery should not be allowed, and also has the burden of clarifying, explaining and supporting its objections with competent evidence.” *Harris v. Best Buy Stores, L.P.*, No. 3:15-cv-00657-HSG (KAW), 2016 WL 6024556, at \*1 (N.D. Cal. Oct. 14, 2016) (quoting *La. Pac. Corp. v. Money Mkt. I Institutional Inv. Dealer*, 285 F.R.D. 481, 485 (N.D. Cal. 2012)). A party claiming undue burden or expense “ordinarily has far better information—perhaps the only information—with respect to that part of the determination.” Fed. R. Civ. P. 26(b)(1) advisory committee’s note (2015). Therefore, the “party claiming that

discovery imposes an undue burden must ‘allege specific facts which indicate the nature and extent of the burden, usually by affidavit or other reliable evidence.’” *Sullivan v. Personalized Media Commc’ns, LLC*, No. 16-MC-80183-MEJ, 2016 WL 5109994, at \*3 (N.D. Cal. Sept. 21, 2016) (quoting *Nationstar Mortg., LLC v. Flamingo Trails No. 7 Landscape Maint. Ass’n*, No. 2:15-cv-01268-RFB-NJK, 2016 WL 4071988, at \*4 (D. Nev. July 28, 2016)).<sup>8</sup> Facebook has furnished no evidentiary support for its objections of undue burden and its objections should be overruled.

Plaintiffs emphasize that they are seeking discovery about *ten Named Plaintiffs*—not millions, not thousands, and not hundreds of users. Based on the information Plaintiffs obtain about themselves, and about Facebook’s general practices and procedures, they will seek to prove their class claims. Facebook’s contention that Plaintiffs are not even entitled to obtain in discovery the evidence necessary to show what Facebook collects about them, and with whom it shares the information is impossible to square with Facebook’s basic discovery obligations under the Federal Rules.

### III. CONCLUSION

For the reasons set forth above, Plaintiffs respectfully request that the Court deny Facebook’s motion to impose a discovery stay and grant Plaintiffs’ motion to compel discovery responsive to Requests for Production Nos. 9 through 13.

---

<sup>8</sup> See also *SPS Techs., LLC v. Briles Aerospace, Inc.*, No. CV 18-9536 MWF (ASx), 2020 WL 4341717, at \*2-3 (C.D. Cal. June 25, 2020) (overruling objection to requests for production of documents and noting that the party resisting discovery must describe “in specific detail, how each Request is overly broad and unduly burdensome by submitting affidavits or other evidence describing the nature of the burden”); *Polaris Innovations Ltd. v. Kingston Tech. Co.*, No. CV1600300CJCRAOX, 2017 WL 3275615, at \*6 (C.D. Cal. Feb. 14, 2017) (court grants motion to compel production of documents by defendant Kingston in part because “[r]egarding its assertion that the requests are overly burdensome, Kingston has not submitted any evidentiary declaration to support this objection.”).

Dated: September 28, 2020

Respectfully submitted,

KELLER ROHRBACK L.L.P.

By: /s/ Derek W. Loeser  
Derek W. Loeser

Derek W. Loeser (admitted *pro hac vice*)  
Lynn Lincoln Sarko (admitted *pro hac vice*)  
Gretchen Freeman Cappio (admitted *pro hac vice*)  
Cari Campen Laufenberg (admitted *pro hac vice*)  
David Ko (admitted *pro hac vice*)  
Benjamin Gould (SBN 250630)  
Adele A. Daniel (admitted *pro hac vice*)  
1201 Third Avenue, Suite 3200  
Seattle, WA 98101  
Tel.: (206) 623-1900  
Fax: (206) 623-3384  
dloeser@kellerrohrback.com  
lsarko@kellerrohrback.com  
gcappio@kellerrohrback.com  
claufenberg@kellerrohrback.com  
dko@kellerrohrback.com  
bgould@kellerrohrback.com  
adaniel@kellerrohrback.com

Christopher Springer (SBN 291180)  
801 Garden Street, Suite 301  
Santa Barbara, CA 93101  
Tel.: (805) 456-1496  
Fax: (805) 456-1497  
cspringer@kellerrohrback.com

Eric Fierro (admitted *pro hac vice*)  
3101 North Central Avenue, Suite 1400  
Phoenix, AZ 85012  
Tel: (602) 248-0088  
Fax: (602) 248-2822  
efierro@kellerrohrback.com

BLEICHMAR FONTI & AULD LLP

By: /s/ Lesley E. Weaver  
Lesley E. Weaver

Lesley E. Weaver (SBN 191305)  
Anne K. Davis (SBN 267909)  
Matthew P. Montgomery (SBN 180196)  
Angelica M. Ornelas (SBN 285929)  
Joshua D. Samra (SBN 313050)  
555 12th Street, Suite 1600  
Oakland, CA 94607  
Tel.: (415) 445-4003  
Fax: (415) 445-4020  
lweaver@bfalaw.com  
adavis@bfalaw.com  
mmontgomery@bfalaw.com  
aornelas@bfalaw.com  
jsamra@bfalaw.com

*Plaintiffs' Co-Lead Counsel*

**ATTESTATION PURSUANT TO CIVIL LOCAL RULE 5-1(i)(3)**

I, Derek W. Loeser, attest that concurrence in the filing of this document has been obtained from the other signatory. I declare under penalty of perjury that the foregoing is true and correct.

Executed this 28th day of September, 2020, at Seattle, Washington.

/s/ Derek W. Loeser

Derek W. Loeser

**CERTIFICATE OF SERVICE**

I, Sarah Skaggs, hereby certify that on September 28, 2020, I electronically filed the foregoing with the Clerk of the United States District Court for the Northern District of California using the CM/ECF system, which shall send electronic notification to all counsel of record.

**In addition, the following were served via email:**

Paven Malhotra  
Matan Shacham  
Bryn Anderson Williams  
pmalhotra@keker.com  
bwilliams@kvn.com  
bwilliams@kvn.com

Anjeza Hassan  
annie.sara@yahoo.com

*/s/ Sarah Skaggs*  
Sarah Skaggs

